UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/654,417	09/04/2003	Philip Kwan	FOUND-0058 (434103-049)	7628

91309 7590 03/24/2010

Nixon Peabody LLP-Brocade
200 Page Mill Road
Suite 200
Palo Alto, CA 94306

EXAMINER	
ABEDIN, SHANTO	
ART UNIT	**PAPER NUMBER**
2436	
MAIL DATE	**DELIVERY MODE**
03/24/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/654,417	KWAN ET AL.	
	Examiner	Art Unit	
	SHANTO M. ABEDIN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 December 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *38-43* is/are allowed.

6)☒ Claim(s) *1-34 and 44-49* is/are rejected.

7)☒ Claim(s) *35-37* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/22/09;02/18/10; 02/22/10*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the communication filed on 12/10/2009.

2. Claims 1-49 have been presented for examination.

3. Claims 35-37 are objected.

4. Claims 38-43 are allowed.

5. Claims 1-34 and 44-49 have been rejected.

Response to Arguments

6. The terminal disclaimer filed on 01/28/2010 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of the US patent application No 10/458628 has been reviewed and is accepted. The terminal disclaimer has been recorded, and the previous obviousness type double patenting rejections are withdrawn.

7. The applicant's arguments regarding the previous 35 USC 103(a) type rejections are fully considered, however, found not persuasive.

Regarding the previous 35 USC 103(a) type rejections, the applicant primarily argues that the cited reference Tsuchiya fails to disclose the limitations such as if the authentication of the physical address indicates the physical address is valid, authenticate user information provided in a second data packet by a user of the user device after the physical address is authenticated.

However, the examiner respectfully notes, upon further examination, the combination of the cited references used in previous 35 USC 103(a) type rejections actually teaches this limitations. For example, upon further examination, the secondary reference Kameda was found to teach the limitations such as if the authentication of the physical address indicates the physical address is valid, authenticate user information provided in a second data packet by a

user of the user device after the physical address is authenticated (Fig 3, steps S32 and S33; Par 053; authenticating the user (step 33) after MAC address is authenticated or matched (step 32.)) Therefore, the previous 35 USC 103(a) type rejections are maintained.

Furthermore, for the sake of addressing the limitations of the amended claims set forth by the arguments, the examiner incorporated a newly found reference US 2002/0016858 A1 (Sawada et al) in this office action, and the amended independent claims 1, 13 and 23 are further rejected applying the reference Sawada et al. Therefore, the applicant's arguments are further moot in view of new grounds of rejections presented in this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-34 and 44-49 are rejected under 35 U.S.C. 103(a) as obvious over Tsuchiya et al (US 7360086 B1) in view of Kameda (US 2003/0028808 A1) further in view of Mao et al (US 7,302,700 B2)

Regarding claim 1, Tsuchiya et al teaches a network access device comprising:

a plurality of input ports (Fig 1.21-25; Col 1, starts at line 25; LAN switch with plural ports);

a memory for storing data packets received on the plurality of input ports (Fig 1.11; Col 2, starts at line 32; network device, switch for storing control/ host table, and port information);

a switching fabric (Fig 1.11; switch) configured for packet switching of the data packets to at least one output port; and

control logic (Col 8, starts at line 5; Col 15,starts at line 24; apparatus); adapted to:

examine a first data packet comprising a physical address of a user device coupled to one of the plurality of input ports (Col 8, starts at line 5; Col 14, lines 10-59; examining data packet containing source/ MAC address information);

authenticate the a physical address (Fig 4, steps 102 and 103; Col 8, starts at line 5; Col 14, lines 10-59; authenticating the MAC address in the host table, or in source information) ; and

if the authentication of the user information indicates the user information is valid ; and restrict further traffic on the one of the plurality of input ports in accordance with the user information (Fig 3; Fig 7; Col 2, lines 32-55;Col 14, lines 40-60; restricting port access based on control, or authentication table)

Tsuchiya et al fails to teach expressly if the authentication of the physical address indicates the physical address is valid, authenticate user information provided in a second data packet by a user of the user device after the physical address is authenticated; and if the network access device has enough system resources to dynamically configure a user policy, dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy.

However, Kameda teaches if the authentication of the physical address indicates the physical address is valid, authenticate user information provided in a second data packet by a user of the user device after the physical address is authenticated (Fig 3, execution of steps S32

and S33; Par 052-054; authenticating the user once/ after MAC address is authenticated or matched) , and to restrict access to the one of the plurality of input ports in accordance with the user information (Fig 1.2 and 51; Par 53-54, 60-62; filtering ports according to the user authentication database.)

Modified Kameda- Tsuchiya et al device fails to teach expressly if the network access device has enough system resources to dynamically configure a user policy, dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy.

However, Mao et al teaches if the network access device has enough system resources to dynamically configure a user policy (Col 4, lines 1-32; Col 5, starts at line 35; generating security policies, and determining whether the policy is associated with the particular virtual private network), dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy (Col 6, line 63- Col 7, line 40; port or address/ VLAN or zone based policies, and processing packets according to the security policies).

Mao et al , Kameda and Tsuchiya et al are analogous art because they are from the same field of endeavor of secure network communication. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to modify Tsuchiya et al 's authentication mechanism with the teachings of Mao et al and Kameda to design a device to dynamically assign a user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy, and wherein authenticate user information provided by a user of the user device only if the physical address is

valid with a reasonable degree of success in order to provide a robust communication control mechanism through user policy.

Regarding claim 13, Tsuchiya et al a computer implemented method (Col 8, starts at line 3; PC, LAN switch) for providing network security, the method comprising:

at a network access device comprising a plurality of input ports (Fig 1.21-25; Col 1, starts at line 25; LAN switch with plural ports) and configured for packet switching of data packets, examining a first data packet comprising a physical address of a user device coupled to one of the plurality of input ports (Col 8, starts at line 5; Col 14, lines 10-59; examining data packet containing source/ MAC address information);

authenticating the physical address (Fig 4, steps 102 and 103; Col 8, starts at line 5; Col 14, lines 10-59; authenticating the MAC address in the host table, or in source information);

if the authentication of the user information indicates the user information is valid ; and restrict further traffic on the one of the plurality of input ports in accordance with the user information (Fig 3; Fig 7; Col 2, lines 32-55;Col 14, lines 40-60; restricting port access based on control, or authentication table)

Tsuchiya et al fails to teach expressly if the authentication of the physical address indicates the physical address is valid, authenticate user information provided in a second data packet by a user of the user device after the physical address is authenticated; and if the network access device has enough system resources to dynamically configure a user policy, dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy.

However, Kameda teaches if the authentication of the physical address indicates the physical address is valid, authenticate user information provided in a second data packet by a user of the user device after the physical address is authenticated (Fig 3, execution of steps S32 and S33; Par 052-054; authenticating the user once/ after MAC address is authenticated or matched) , and to restrict access to the one of the plurality of input ports in accordance with the user information (Fig 1.2 and 51; Par 53-54, 60-62; filtering ports according to the user authentication database.)

Modified Kameda- Tsuchiya et al method fails to teach expressly if the network access device has enough system resources to dynamically configure a user policy, dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy.

However, Mao et al teaches if the network access device has enough system resources to dynamically configure a user policy (Col 4, lines 1-32; Col 5, starts at line 35; generating security policies, and determining whether the policy is associated with the particular virtual private network), dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy (Col 6, line 63- Col 7, line 40; port or address/ VLAN or zone based policies, and processing packets according to the security policies).

Mao et al , Kameda and Tsuchiya et al are analogous art because they are from the same field of endeavor of secure network communication. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to modify Tsuchiya et al 's authentication mechanism with the teachings of Mao et al and Kameda to design a method to dynamically assign a user policy to the one of the plurality of input ports and restrict further

traffic on the one of the plurality of input ports in accordance with the user policy, and wherein authenticate user information provided by a user of the user device only if the physical address is valid with a reasonable degree of success in order to provide a robust communication control mechanism through user policy.

Regarding claim 23, Tsuchiya et al teaches a network system, comprising:

a network access device comprising a plurality of input ports and configured for packet switching of data packets in a data communications network (Fig 1.21-25; Col 1, starts at line 25; LAN switch with plural ports); and

a user device coupled to a port of the network access device (Fig 1; Col 8, starts at line 2; PC and LAN switch);

wherein the network access device (Fig 1; LAN Switch) is adapted to:

examine a first data packet comprising a physical address of a user device coupled to one of the plurality of input ports (Col 8, starts at line 5; Col 14, lines 10-59; examining data packet containing source/ MAC address information);

authenticate the a physical address (Fig 4, steps 102 and 103; Col 8, starts at line 5; Col 14, lines 10-59; authenticating the MAC address in the host table, or in source information) ; and

if the authentication of the user information indicates the user information is valid ; and restrict further traffic on the one of the plurality of input ports in accordance with the user information (Fig 3; Fig 7; Col 2, lines 32-55;Col 14, lines 40-60; restricting port access based on control, or authentication table)

Tsuchiya et al fails to teach expressly if the authentication of the physical address indicates the physical address is valid, authenticate user information provided in a second data

packet by a user of the user device after the physical address is authenticated; and if the network access device has enough system resources to dynamically configure a user policy, dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy.

However, Kameda teaches if the authentication of the physical address indicates the physical address is valid, authenticate user information provided in a second data packet by a user of the user device after the physical address is authenticated (Fig 3, execution of steps S32 and S33; Par 052-054; authenticating the user once/ after MAC address is authenticated or matched) , and to restrict access to the one of the plurality of input ports in accordance with the user information (Fig 1.2 and 51; Par 53-54, 60-62; filtering ports according to the user authentication database.)

Modified Kameda- Tsuchiya et al system fails to teach expressly if the network access device has enough system resources to dynamically configure a user policy, dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy.

However, Mao et al teaches if the network access device has enough system resources to dynamically configure a user policy (Col 4, lines 1-32; Col 5, starts at line 35; generating security policies, and determining whether the policy is associated with the particular virtual private network), dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy (Col 6, line 63- Col 7, line 40; port or address/ VLAN or zone based policies, and processing packets according to the security policies).

Mao et al , Kameda and Tsuchiya et al are analogous art because they are from the same field of endeavor of secure network communication. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to modify Tsuchiya et al 's authentication mechanism with the teachings of Mao et al and Kameda to design a system to dynamically assign a user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy, and wherein authenticate user information provided by a user of the user device only if the physical address is valid with a reasonable degree of success in order to provide a robust communication control mechanism through user policy.

Regarding claim 2, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches the network access device wherein the physical address comprises a Media Access Control (MAC) address (Col 1, starts at line 25; MAC address).

Regarding claim 3, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches the network access device wherein the control logic is adapted to authenticate the user information (Fig 3; Col 2, starts at line 32). Tsuchiya et al fails to teach utilizing IEEE 802. lx protocol. However, examiner takes an official notice on that at the time of invention, use of IEEE 802. lx protocol in wireless/ VLAN security was well known in the art (see US 7188364 B2). Therefore, it would have been obvious to an ordinary skill in the art to design the authentication mechanism accordance with the IEEE 802. lx protocol in order to provide an alternative and robust authentication mechanism.

Regarding claim 4, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches the network access device wherein the user policy identifies an access control list (Fig 3; Col 2, starts at line 35; authentication unit utilizing control, or authentication table, or host table).

Regarding claim 5, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches the network access device wherein the user policy includes an access control list (Fig 3; Col 2, starts at line 35; control, or authentication table).

Regarding claim 6, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches the network access device wherein the user policy identifies a Media Access Control (MAC) address filter (Fig 2; MAC address in host table). Furthermore, Kameda teaches the network access device wherein the user policy identifies a Media Access Control (MAC) address filter (Fig 1.22; MAC address filter in switch table)

Regarding claim 7, it is rejected applying as above applied rejecting claim 1, furthermore, Kameda teaches the network access device wherein the user policy includes a Media Access Control (MAC) address filter (Fig 1.22; MAC address filter in switch table).

Regarding claim 8, it is rejected applying as above applied rejecting claim 1, furthermore, Kameda teaches the device wherein the control logic is adapted to send user information to an authentication server and to receive an accept message from authentication server if the user information is valid (Fig 1; authentication server; Fig 1.2 and 51; Par 53-54, 60-62; assigning/ filtering ports, MAC addresses according to the authentication database).

Regarding claim 9, it is rejected applying as above applied rejecting claim 1, furthermore, Kameda teaches the network access device wherein the authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server (Fig 1; Par 012,037; remote authentication server).

Regarding claim 10, it is rejected applying as above applied rejecting claim 9, furthermore, Kameda teaches the network access device wherein the accept message includes the user policy (Fig 1; authentication server table including authentication response information; Fig 1.2 , 5 and 51; Par 53-54, 60-62; server authentication database)

Regarding claim 11, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches the network access device wherein the control logic is further adapted to assign the one of the plurality of input ports to a virtual local area network (VLAN) associated with the user information if the user information is valid (Fig 2; Col 1, starts at line 16; authenticating VLAN information).

Regarding claim 12, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches the network access device wherein the control logic is adapted to receive a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information, and to assign the one of the plurality of input ports to a VLAN associated with the VLAN ID (Fig 2; Col 1, starts at line 16; authenticating VLAN information/ number).

Regarding claim 44, it is rejected applying as above applied rejecting claim 1, furthermore, Tsuchiya et al teaches the device wherein the user information comprises a user name and a password (Fig 3; Col 8, lines 40-50)

Regarding claim 47, it is rejected applying as above applied rejecting claim 1, furthermore, Mao et al teaches the network access device wherein the control logic is further adapted to: if the authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol (Col 10, starts at line 17; processing of the probe packet.)

Regarding claims 14-22, 24-34, 45-46 and 48-49, they recite the limitations of claims 1-13, 23, 44 and 47, therefore, they are rejected applying as above applied rejecting claims 1-13, 23, 44 and 47.

9. Claims 1, 13 and 23 are further rejected under 35 U.S.C. 103(a) as obvious over Sawada et al (US 2002/0016858 A1) in view of Mao et al (US 7,302,700 B2)

Regarding claims 1 and 13, Sawada et al discloses a network access device (Par 082-084, 092, 095-100 ; LAN switch), or a computer implemented method (Par 079, 082 ; LAN switch/ terminal) comprising:

a plurality of input ports (Par 083, 097 ; switch/ receiving ports) ;

a memory for storing data packets received on the plurality of input ports (Par 089, 129 ; switch/ server for receiving and storing of packets);

a switching fabric configured for packet switching of the data packets to at least one output port (Par 075, 083, 092, 097 ; forwarding packets through sending port); and

control logic adapted to:

examine a first data packet comprising a physical address of a user device coupled to one of the plurality of input ports (Fig 6 ; Fig 32 ; Par 089 ; examining for MAC address);

authenticate the a physical address (Fig 6 ; Fig 32 ; Par 089, 231 ; authenticating/ matching of the MAC address);

if the authentication of the physical address indicates the physical address is valid, authenticate user information provided in a second data packet by a user of the user device after the physical address is authenticated (Fig 5.501 and 502 ; Fig 32.3201 and 3204 ; Fig 34.3401 and 3405 ; Par 200, 269 ; authenticating user password/ ID, or IP address after MAC address being authenticated/ matched.)

Sawada et al fails to disclose expressly if the authentication of the user information indicates the user information is valid and if the network access device has enough system resources to dynamically configure a user policy, dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy.

However, Mao et al teaches if the authentication of the user information indicates the user information is valid and if the network access device has enough system resources to dynamically configure a user policy (Col 4, lines 1-32; Col 5, starts at line 35; generating security policies, and determining whether the policy is associated with the particular virtual private network), dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy (Col 6, line 63- Col 7, line 40; port or address/ VLAN or zone based policies, and processing packets according to the security policies).

Mao et al and Sawada et al are analogous art because they are from the same field of endeavor of authenticating a secure network communication. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Mao et al with Sawada et al to design a device/ method further including the feature such as if the authentication of the user information indicates the user information is valid and if the network access device has enough system resources to dynamically configure a user policy, dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy in order to provide a robust communication control mechanism using a user policy.

Regarding claim 23, Sawada et al discloses a network system, comprising:

a network access device (Par 076, 089, 097 ; LAN switch) comprising a plurality of input ports and configured for packet switching of data packets in a data communications network (Par 075, 083, 092, 097 ; receiving/ forwarding packets through receiving/ sending port); and

a user device coupled to a port of the network access device (Par 089, 097 ; user terminal comunicating with the switch);

wherein the network access device (Par 076, 089, 097 ; LAN switch) is adapted to:

examine a first data packet comprising a physical address of a user device coupled to one of the plurality of input ports (Fig 6 ; Fig 32 ; Par 089 ; examining for MAC address);

authenticate the a physical address (Fig 6 ; Fig 32 ; Par 089, 231 ; authenticating/ matching of the MAC address);

if the authentication of the physical address indicates the physical address is valid, authenticate user information provided in a second data packet by a user of the user device after the physical address is authenticated (Fig 5.501 and 502 ; Fig 32.3201 and 3204 ; Fig 34.3401 and 3405 ; Par 200, 269 ; authenticating user password/ ID, or IP address after MAC address being authenticated/ matched.)

Sawada et al fails to disclose expressly if the authentication of the user information indicates the user information is valid and if the network access device has enough system resources to dynamically configure a user policy, dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy.

However, Mao et al teaches if the authentication of the user information indicates the user information is valid and if the network access device has enough system resources to dynamically configure a user policy (Col 4, lines 1-32; Col 5, starts at line 35; generating security policies, and determining whether the policy is associated with the particular virtual private network), dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy (Col 6, line 63- Col 7, line 40; port or address/ VLAN or zone based policies, and processing packets according to the security policies).

Mao et al and Sawada et al are analogous art because they are from the same field of endeavor of authenticating a secure network communication. Therefore, at the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Mao et al with Sawada et al to design a device/ method further including the feature such as if the authentication of the user information indicates the user information is valid and if the network access device has enough system resources to dynamically configure a user policy, dynamically assign the user policy to the one of the plurality of input ports and restrict further traffic on the one of the plurality of input ports in accordance with the user policy in order to provide a robust communication control mechanism using a user policy.

Allowable Subject Matter

10. Claims 35-37 would be allowable if rewritten to include all of the limitations of the base claim and any intervening claims.

11. Claims 38-43 are allowed.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 10:00 AM to 6:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195.

The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/SHANTO M ABEDIN/

Examiner, Art Unit 2436

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436